AUTOMATIC HUMAN PROFILE VERIFICATION SYSTEM

Mohamed Mamdouh, Emad M.Rasmy, Mohamed Sheren and Sherif Samy
Biomedical Engineering Dept., Cairo University, Giza, Egypt
E-mail: m_mamdouh75@yahoo.com

Abstract- **Automatic human identification by biometric methods has been carried out in many ways, such as fingerprint recognition, signature recognition, face recognition, hand geometry recognition, speed recognition, retina vessel recognition and ear recognition. Face recognition is from the important branch of automatic human identification, since the early 1960's face recognition become an active research area. In face recognition, face profile images are important aspect for the recognition of faces, which provides a complementary and detailed structure of the face that is not seen in the frontal images. Though it contains less discriminating power than frontal images, it is relatively easy to analyze and more foolproof. We introduce a new technique for the efficient extraction of the human profile characteristic. This feature is the length of curve which expresses of the nose of human profile. This feature is extracted from the plan of the 2D human profile image captured by a digital camera with 480x640 resolutions.**
Keywords **- recognition, profile, verification, identification, Biometric**

I. INTRODUCTION

Human use physical characteristics or behavioral traits to identify human individuals. With the development of the life and the complex of the society, we need an easy and a fast human identification tools in different areas such as national security, business and research areas. So that, over a century and till now the human recognition such as identification and verification becomes an active research area. Verification (authentication) refers to confirm or deny a person's claimed identity (Am I who I claim I am?). Identification (Who am I?) refers to establish a subject's identity.

The techniques for automatically identifying an individual based on physiological characteristics are called biometrics, which provides our needing for easy and fast human identification tools. Biometrics techniques fall into two categories: physiological and behavioral. Common physiological biometrics includes face, eye (retina or iris), ear, fingerprint, finger (fingertip, thumb, finger length or pattern), palm geometry and hand geometry. Behavioral biometrics includes speech, signatures, signature dynamics and human motion. Behavioral biometric technologies are less robust than physical biometric systems [1].

Human face recognition remains one of the important branches of automatic human recognition in biometrics, despite the existence of alternative technologies such as fingerprint or iris recognition. The major reason for this is the non-intrusive nature of face recognition methods, which makes them a wide range of application especially suitable to tracking applications. Other biometric methods do not possess these advantages. For instance, iris recognition methods require the users to place their eyes carefully relative to a camera [2], [3]. Similarly, fingerprint recognition methods require the users to make explicit physical contact with the surface of a sensor [2], [4].

Nevertheless, despite the above-mentioned advantages of face recognition as a method of biometric identification, there are some issues that can seriously affect the performance of a face recognition system. The appearance of the human face is subject to several different changes owing to a combination of factors such as head pose, expressions, illumination, occlusions, and make-up. To be of use in the real world, a face recognition system should be robust to such changes. Face recognition has been performed using 2D images of a person [2].

Since the early 1960's face recognition become an active research area. The development of face recognition over the past years allows an organization into three types of recognition algorithms, namely frontal, profile, and view-tolerant recognitions, depending on both the kind of imagery (facial views) available, and on the according recognition algorithms. While face profile image is important aspect for the other recognition of faces, which provides a complementary and detailed structure of the face that is not seen in the frontal and view-tolerant images [5]. Though it contains less discriminating power than the others, it is relatively easy to analyze and more foolproof.

In the modern world, there is an ever-growing need to authenticate and identify individuals automatically. The current technologies of using a PIN or password for these purposes are inadequate because they are disclosable, transferable and hard to remember. Biometric-based authentication and identification methods are emerging as the most reliable. Automated biometrics deal with physiological or behavioral characteristics such as fingerprints, voice and face that can be used to authenticate a person's identity or establish an identity within a database. With rapid progress in electronic and Internet commerce, there is also a growing need to authenticate the identity of a person for secure transaction processing. So that, the goal of this thesis is to use the information available in biometric techniques, image processing and pattern recognition implementation in realizing an Automatic Human Face Profile Verification System (APVS) which should be robust to such changes in the environment surround or human behavioral. This system realizes a measure of person's identifying based on feature extraction stage. This feature is the length of nose curve of every person. This feature in human profile is robust to such changes than the other features in human profile such as forehead, lips and chin.

II. METHODOLOGY

The facial recognition method analyses the patterns in individual faces. Similar to the way in which we recognize friends and family amongst a group of people by focusing on their faces, a facial recognition biometric system takes images from standard capture techniques such as digital

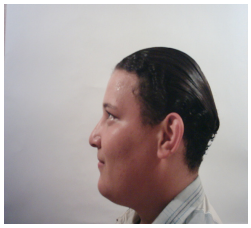

Figure 2.1: Profile Recognition

pictures and generates a mathematical representation of the human face. This is compared to a template or set of templates, held electronically on a central system, to authenticate or identify an individual.

The Automatic Human Profile Verification System (APVS) consists of four stages as following:

1) Data acquisition stage:

Is the first stage in the Automatic Human Profile Verification System (APVS), where acquiring the human face profile images takes place. Images are captured by a digital camera in 480x640 resolutions (RGB) format.

2) Pre-processing stage

It is the second stage in the Automatic Human Profile Verification System (APVS). It mainly consists of four consecutive sub stages, namely, color edge detection sub stage, binarization sub stage, boundary detection sub stage and boundary tracing sub stage, we used the color gradient for RGB image to detect the edge This technique is suitable of our application because this method applicable in 2-D space but doesn't extend to higher dimensions [10].

The following function implements the color gradient for RGB images:

[VG, A, PPG] = colorgrad (f, T)

f: is the RGB image; T: is an optional threshold in the range [0, 1]; VG: is the RGB vector gradient; A: is the angle image; PPG: is the gradient formed by summing the 2-D gradients of the individual color planes; colorgrad: is the MATLAB function of the color gradient.

After that the binarization step is one of the most steps in image processing techniques leading to divide the image into two levels; the object (human profile) and background; the object segment which is the human profile in 1-binary digit (white) and the background segment in 0-binary digit (black).

The boundary detection is the next sub stage after binarization takes place. It is done by examining the white pixels and the 8-neighborhood pixels around it, if the pixel is white, and all its 8-neighborhood pixels are black, then the central pixel is noisy pixel, and it is changed to black, otherwise it is a boundary pixel and it remains white. But if the pixel is white, and all its 8-neighborhood pixels are white then the central pixel is an interior pixel in the objective (the human profile) and it is changed to black, otherwise it is a boundary pixel and it remains white.

Tracing the boundary of the human profile to construct a x-y array for the human profile boundary in sequence.

3) Analysis stage

This stage is the third stage in the Automatic Human Profile Verification System (APVS), this stage is four steps: (1) find maximum and minimum points on 1D, (2) Find concave and convex shapes in 2D, (3) Feature extraction stage, (4) Matching stage.

This step is used to convert the boundary of human profile curve from 2D to 1D based on angles between vectors. The approaches that have been proposed to estimate the angle by vectors along the boundary of human profile. These vectors are defined between the current point and the numbers of neighbor's points to the left and to the right of the boundary curve of the human profile. And then, we can find the maximum and minimum points along the boundary curve of the human profile 1D. After the maximum and the minimum points are indicated on the 1D curve of the human profiles, we use the coordinate of these points to indicate on the 2D boundary curve of the human profile, so the concave and the convex shapes are appeared on the curve. Feature extraction stage is the third step of the analysis stage. Finally we normalize the nose curve; the normalizing stage consists of four steps: 1) translation, 2) scaling, 3) rotation, 4) equal distance. At the end of this step, a human profile feature becomes available to be passed to the matching stage, where it is compared with the biometric template which is stored in the database.

4) Matching stage:

This stage is compared the feature which is extracted, with the biometric templates which are stored in the database, to generate a decision, whether this human profile is for the same person or not.

III. Results and Discussion

As for any biometric system, the Automatic Human Profile Verification system (APVS) consists of both hardware and software; the hardware captures the salient human characteristic which is the human face profile. The software consists of the algorithms and programs; the algorithms and programs are implemented using MATLAB version 7.0 as a mathematical computer environment with different tool boxes such as Image processing and Signal processing.

Finally, the technique that is introduced and implemented are tested using 600 human profile images for 100 persons from the general public in different ages, and the Automatic Human Profile Verification System (APVS) is given 99.26 % rate of success.

V. Conclusion

Biometric is a hot topic, and biometric technologies are potentially of significance in a range of security, access control and monitoring applications. The technologies are still new and rapidly evolving. In recent years, the price of microprocessors and advanced imaging electronics has dropped dramatically while the accuracy of biometrics devices has increased. Thus Automatic Human Profile Verification System in becoming more popular especially in the area of access control.

In most biometric-security applications, you do not ask the system to determine the identity of the person who presents himself to the system. That is, you not say to the

system, "of the millions of sets of sets of patterns you have in file, which set contains a pattern that matches this one? "This problem is "one-to many matching." Usually, you supply your identity to the system, and ask the system to confirm that you are who you say you are. This problem is "one to one matching."Today's PCs can conduct a one-to-one match in, at most, a few seconds.

The body offers uniquely recognizable feature in the following areas: fingerprints, voice, eyes, hands and face different vendors are developing products around each of these features, and the jury is very much out on which technology is best. Success is measured according to a number of criteria, and each technology has both strengths and weakness.

The most important criteria are concerned with accuracy, the level of accuracy in biometric systems involves both the false accept rate (FAR) and false reject rate (FRR). These rates are useful, and the biometric product vendors often cite them in their product descriptions. But they don't present a complete picture. The fact is, people's physical traits change over time, especially with alterations due to accident or aging. And even in the short term, problems can occur because of humidity in the air, dirt and sweat on the user (especially with fingerprint system), and inconsistent ways of interfacing with the system, such as not taking enough time for the system to make an accurate identification. And users of biometric systems, like the users of all systems, must be trained to use them most efficiently.

These and other issues limit the accuracy of biometric devices. But there is little doubt that biometric systems are more accurate than other kinds of security systems, because they are based on users' actual physical characteristics, not on what they know (as with passwords) or what they are carrying (such as ID badges).

Biometric success is also judged via a number of other factors. Vulnerability to fraud, also known as barrier to attack, reflects how likely it is that a person can fraudulently get past the security. Long-term stability deals with issues such as whether a system is useful for very infrequent users, as well as whether or not user's characteristics alter over time. other effectiveness measures can include factors that might interfere with the system, ease, and the size of the system and the amount of disk space its data takes up.

Just which biometric technologies are best for particular applications have become the subject of heated debates. And what increases this debate, is the lack of objective information comparing the accuracy of the various technologies. Factors that add interest to the comparing include the ease of use, the likelihood of public acceptance, and the ease with which someone intent on deception can fool a technique.

The issue of likelihood is central to discussions of biometrics. No system can be 100%-accurace. The goal is to make fooling the system so complex and expensive that would be attackers decide that the potential rewards do not justify the required effort. Still, the idea of combining multiple biometric technologies into one system is at the heart of another debate among biometrics advocates.

It is clear that a number of biometric modalities working together can result in increased performance, reliability and ease of use. There is therefore considerable interest in developing multi-modal and layered systems.

Despite its problems, biometric security offers several advantages over current approaches. People can steal or copy keys. Badges used to control admission to secure areas are of no value unless they require you to enter a PIN. You can too easily forget your password or PIN, and if you write it down, someone else may find it and misuse it.

Of course, this is partly what passwords have done all along. Passwords determine identity through user knowledge: If you know the password, you can access to the System. The problem is that a password has nothing to do with your actual identity. Passwords can be stolen, and users can give their passwords to others, resulting in a system that is far too open to too many people. There is simply no foolproof way to make password-protected systems completely safe from unauthorized intrusion. Also there is no any way for password-based systems to determine user identity beyond doubt.

Finally we can say "Really with Biometrics, you are your Password"

REFERENCES

[1] Nader Shaaban, “A Prototype of Automatic Hand Geometry Verification System”, M.Sc thesis, Cairo University, May 2002.

[2] Ajit Rajwade, “Facial Pose Estimation and Face Recognition from Three-Dimensional Data”, MSc thesis, McGill University, August 2004.

[3] “The Iris Recognition Homepage”, http://www.iris-recognition.org/

[4] D. Maltoni, D. Maio, A. Jain and S. Prabhakar, “Handbook of Fingerprint Recognition”, Springer Verlag, 2003.

[5] Thomas Fromherz, “Face Recognition: a Summary of 1995 – 1997”, International Computer Science Institute, fromherz@icsi.berkeley.edu

[6] Xiaoguang Jia, “Extending the Feature Set for Automatic Face Recognition”, PhD thesis, University of Southampton, 1993.